(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 743 864 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.06.2014 Bulletin 2014/25

(51) Int Cl.:
G06K 19/077 *(2006.01)* ***G09F 3/03*** *(2006.01)*

(21) Application number: **12197521.3**

(22) Date of filing: **17.12.2012**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(71) Applicant: **Nafith Logistics Psc.**
11821, Amman (JO)

(72) Inventor: **Mubarak, Sameer**
11190 Amman (JO)

(74) Representative: **Calvo de Nó, Rodrigo et al**
Cabinet Beau de Loménie
158, rue de l'Université
75340 Paris Cedex 07 (FR)

(54) Secure sealing device and method

(57) The present invention concerns a secure sealing device 101 comprising at least a closure element 102 with an electrically conductive path 120, and a locking body 103 comprising an electric circuit with a data carrier and a radiofrequency transceiver with a predetermined working wavelength. Said locking body 103 is configured to lock together a first and a second end 102a, 102b of said closure element 102 to attach the locking body 103 to an object to be sealed. The electrically conductive path 120 of the closure element 102 has a length which is substantially equal to a multiple of half said predetermined working wavelength of the radiofrequency transceiver, thus enhancing the range of the radiofrequency transceiver by inductive coupling.

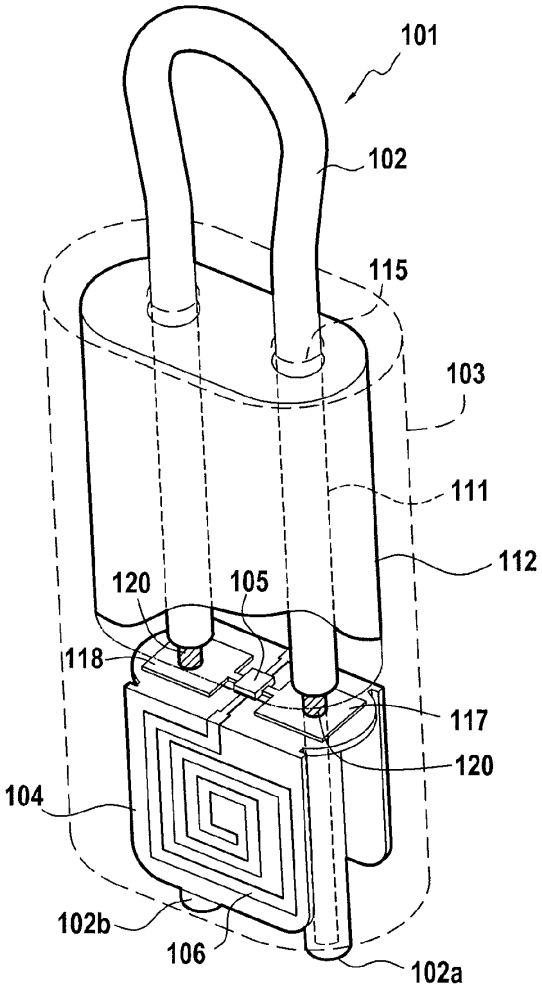


FIG.1

EP 2 743 864 A1

Description

TECHNICAL FIELD

[0001] The invention relates to the domain of secure sealing devices and methods, in particular those involving transceivers.

BACKGROUND

[0002] It has been a long-standing human necessity to seal access to certain assets, in particular assets in transit. In order to prevent smuggling, for instance, customs authorities routinely seal in-transit cargo vehicles and shipping containers with tagged sealing devices. Such tagged sealing devices may also be used by cargo owners or logistics providers to protect cargo against theft or other unauthorized tampering. While the physical protection offered by such tagged sealing devices may be limited, their main purpose is to clearly reveal whether they have been breached and the cargo potentially accessed. By regularly checking the tagged sealing devices, the cargo can be tracked and, if the sealing device has been breached, it is possible to identify the transit segment during which the breach has taken place. Such tagged sealing devices can thus be very efficient deterrents against unauthorized access, diversion and/or tampering of assets in transit.

[0003] Different types of tagged sealing devices are known to the skilled person. In one of its simplest forms, such a tagged sealing device may be a plastic tag with a ratchet strap. More elaborate tagged sealing devices take the form of a metal lock with a wire strap, a tagged metal strip seal, or a tagged bolt seal. To prevent false alerts, it is also important to prevent accidental breaches of such tagged sealing devices. To this purpose, the International Standard Organization (ISO) has issued the ISO 17712 standard for Tensile, Shear, Bend and Impact Resistance certification for sealing devices.

[0004] One inconvenience of most such tagged sealing devices is that checking and identifying them requires close visual inspection of the tags. When large numbers of containers have to be tracked, for instance in important customs checkpoints or transshipment facilities, this can be extremely tedious and time-consuming. Moreover, agents visually inspecting large numbers of seals may easily overlook individual seal breaches.

[0005] For this reason, several different types of secure sealing devices have been proposed incorporating radiofrequency identification (RFID) technology. Such RFID devices incorporate a radiofrequency transceiver for wirelessly communicating identification data to a remote reader. Moreover, the radiofrequency transceiver may also transmit a specific signal if the sealing device has been breached. For instance US Patent Application Publications US 2005/0231365 A1 and US 2007/0103310 A1 and US Patent US 6,265,973 B1 each disclose a secure sealing device with an electronic circuit configured to transmit a specific signal in case of breach. However, the secure sealing devices disclosed in these documents require active radiofrequency transceivers, and thus a power supply. Ensuring such a power supply increases the complexity and cost of these sealing devices and reduces their reliability. The range at which such secure sealing devices can respond to a remote reader depends on this power supply. Increasing this range thus normally involves a trade-off in terms of increasing cost and decreasing reliability.

[0006] Alternatively, secure sealing devices have also been proposed that only require a passive radiofrequency transceiver, that is, a transceiver that can be powered solely by the energy of incoming radio signals. Such devices have been disclosed in US Patent Application Publications US 2006/0145868 A1, US 2006/0087431 A1 and US 2007/0139196 A1. In these secure sealing devices, an electrically conductive path connecting the radiofrequency transceiver and antenna is broken if the seal is breached. Such a breach can therefore be easily detected. However, one drawback of these secure sealing devices is that the range at which they respond to a remote reader is normally quite limited.

SUMMARY

[0007] A first object of the disclosure is that of providing a simple and tamper-safe secure sealing device, and in particular a secure sealing device comprising at least a closure element with an electrically conductive path, and a locking body comprising an electric circuit with a data carrier and a radiofrequency transceiver with a predetermined working wavelength, said locking body being also configured to lock together a first and a second end of said closure element to attach the locking body to an object to be sealed, wherein the communication range of the radiofrequency transceiver with a remote reader is significantly increased without requiring an increased internal or external power supply.

[0008] For this purpose, in at least one illustrative embodiment, the electrically conductive path of the closure element has a length which is substantially equal to a multiple of half said predetermined working wavelength of the radiofrequency transceiver. With this length, this electrically conductive core can work as a supplemental antenna at said working wavelength of the closure element, significantly increasing the range of the radiofrequency transceiver by inductive coupling, even without being physically connected to it. Within the present length, "substantially equal" is understood as allowing a variation of, for example, $\pm 10\%$ with respect to said working wavelength.

[0009] This inductive coupling of the electrically conductive core of the closure element with the radiofrequency transceiver can be enhanced if the radiofrequency transceiver comprises at least a first planar antenna oriented in a first plane, and said locking body is configured to lock together said first and second ends of the closure

element oriented in a plane substantially parallel to said first plane. The electrically conductive path of the closure element and the first planar antenna can thus be oriented along substantially parallel planes, which facilitates their inductive coupling. For better coverage to each side of the secure sealing device, the radiofrequency transceiver may comprise at least a second planar antenna oriented substantially parallel to the first planar antenna. "Substantially parallel" is understood as being functionally equivalent to a parallel orientation, although there may be a slight divergence, for instance of 5° or 10°.

[0010] A second object of the present disclosure is to provide a secure sealing device which is tamper-proof, in particular against a breach of the closure element. For that purpose, said electric circuit may comprise first and second electric terminals configured to be connected through the electrically conductive path of the closure element when the first and second ends of the closure element are locked together by the locking body, so that a breach of the closure element will interrupt this connection between the first and second electric terminals, interruption that may be easily detected by the electric circuit. In particular, the electric circuit may be configured to automatically store within said data carrier whether a connection between said first and second electric terminals has been interrupted. With this further anti-tampering feature, it will be possible to identify a breached seal even if the connection has been subsequently reestablished.

[0011] It is a third object of the present disclosure to provide a particularly compact secure sealing device. For this purpose, the electric circuit may be formed onto a substrate comprising at least a first segment, supporting at least a first planar antenna of the radiofrequency transceiver, extending in a first plane, and a second segment, supporting at least said first and second terminals and extending in a second plane at an angle, for example a substantially straight angle, with respect to the first plane. For better coverage to either side of the secure sealing device, the substrate may further include a third segment, supporting at least a second planar antenna of the radiofrequency transceiver, and extending substantially parallel to the first segment. To protect the electric circuit against accidental damage or tampering, the electric circuit may be encased within a dielectric material. Within the present disclosure, "substantially straight angle" is understood as an angle which, for its present practical purpose, is functionally equivalent to a straight angle, although it may differ slightly from 90°, for instance by 5° or 10°. It must be noted that these features of the electric circuit can be used even in isolation of other features of the disclosure, and at least some of their advantages enjoyed even in an analogous secure sealing device in which the closure element does not present an electrically conductive path, or its electrically conductive path is of a length which is not substantially equal to a multiple of half a working wavelength of the radiofrequency transceiver.

[0012] In order to physically impede an intentional or accidental seal breach, said locking body may comprise at least a first opening for insertion of the first end of said closure element into said locking body, and a first holding mechanism for preventing removal of said first end from said first opening once inserted.

[0013] Analogously, the locking body may also comprise a second opening for insertion of the second end of said closure element into said locking body, and a second holding mechanism for preventing removal of said second end from said second opening once inserted. Alternatively, however, the second end of the closure element may be solid with the locking body, so that it does not require to be inserted or locked into it.

[0014] To facilitate the use of the secure sealing device, the closure element may be flexible. Alternatively, however, it may be rigid, as in a padlock.

[0015] In order to increase the versatility of the secure sealing device, and in particular to adapt it to a plurality of different standards, its radiofrequency transceiver may have a plurality of predetermined working wavelengths, and its closure element a plurality of electrically conductive paths of different lengths, each one substantially equal to a multiple of one half of one of said plurality of predetermined working wavelengths of the radiofrequency transceiver.

[0016] It is a further object of the present disclosure to provide a method for checking the integrity of such a secure sealing device. For this purpose, an external reader, located at a predetermined range from said radiofrequency transceiver, may send an interrogation signal, addressed to the radiofrequency transceiver and using said working wavelength, at various different transmission power levels, and issue an alert if it fails to receive a response of the radiofrequency transceiver below a predetermined transmission power threshold of the interrogation signal. This "power sweep" technique allows a fast and easy first remote check of the integrity of the secure sealing device.

[0017] The above summary of some example embodiments is not intended to describe each disclosed embodiment or every implementation of the invention. In particular, selected features of any illustrative embodiment within this specification may be incorporated into an additional embodiment unless clearly stated to the contrary.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] The invention may be more completely understood in consideration of the following detailed description of various embodiments in connection with the accompanying drawings, in which :

- FIG. 1 is a cutaway perspective view of a secure sealing device according to a first embodiment of the present invention ;
- FIG. 2 is a perspective view of an RFID inlay of the

secure sealing device of FIG. 1 ;

- FIG. 3 is a transversal cut view of the closure element of the secure sealing device of FIG. 1 ;
- FIG. 4 is a cutaway perspective view of a secure sealing device according to a second embodiment of the present invention ;
- FIG. 5 is a perspective view of an RFID inlay of the secure sealing device of FIG. 4 ;
- FIG. 6 is a cutaway perspective view of a secure sealing device according to a third embodiment of the present invention ;
- FIG. 7 is a perspective view of an RFID inlay of the secure sealing device of FIG. 6 ;
- FIG. 8A is a perspective view of a secure sealing device according to a fourth embodiment of the present invention; and
- FIG. 8B is a cutaway perspective view of the secure sealing device of FIG. 8A ; and
- FIG. 9 is a perspective view of an RFID inlay of the secure sealing device of FIGS. 8A and 8B.

[0019] While the invention is amenable to various modifications and alternative forms, specifics thereof have been shown by way of example in the drawings and will be described in detail. It should be understood, however, that the intention is not to limit aspects of the invention to the particular embodiments described. On the contrary, the intention is to cover all modifications, equivalents, and alternatives falling within the scope of the invention.

DETAILED DESCRIPTION

[0020] For the following defined terms, these definitions shall be applied, unless a different definition is given in the claims or elsewhere in this specification.

[0021] As used in this specification and the appended claims, the singular forms "a", "an", and "the" include plural referents unless the content clearly dictates otherwise. As used in this specification and the appended claims, the term "or" is generally employed in its sense including "and/or" unless the content clearly dictates otherwise.

[0022] The following detailed description should be read with reference to the drawings in which similar elements in different drawings are numbered the same. The detailed description and the drawings, which are not necessarily to scale, depict illustrative embodiments and are not intended to limit the scope of the invention. The illustrative embodiments depicted are intended only as exemplary. Selected features of any illustrative embodiment may be incorporated into an additional embodiment unless clearly stated to the contrary.

[0023] A secure sealing device 101 according to a first embodiment of the present invention is illustrated in FIG. 1. This secure sealing device 101 comprises a closure element 102 and a locking body 103. In the illustrated embodiment, the closure element 102 is an elongated, flexible cord with an electrically conductive path 120, such as can be produced by winding together a core of several strands of electrically conductive filaments, covered by an electrically insulating sheath 121. As illustrated in FIG. 3, the closure element 102 has a round cross-section, although other cross-sections, for example polygonal cross-sections, can alternatively be considered. First and a second channels 111 each traverse the locking body 103, including a locking core 112 with respective holding mechanisms for locking each end 102a, 102b of the closure element 102.

[0024] For visual identification of the secure sealing device 101, the locking body 103 can present visible markings (not shown), in the form, for instance, of alphanumeric codes, bar codes, or other human- or machine-readable codes, printed or embossed, or of other authentication or identification markings, such as, for instance, holograms.

[0025] However, as illustrated in FIGS. 1 and 2, the secure sealing device 101 also comprises, embedded within the locking body 103, an RFID inlay 104 carrying an electric circuit comprising a data carrier, a transceiver, first and second antennas 106,107 for the transceiver, and first and second electric terminals 117,118. In this first embodiment, the data carrier and transceiver are integrated in an RFID integrated circuit 105, compliant with ISO/IEC 18000 and bonded onto the RFID inlay 104. The working frequencies of this RFID integrated circuit 105 may be, for instance, 2.45 GHz, as specified under ISO/IEC 18000-4, 860-960 MHz, as specified under ISO/IEC 18000-6, and/or 433 MHz, as specified under ISO/IEC 18000-7. The data carrier can be a read-only or a rewritable memory, wherein a rewritable memory could store information received by the radiofrequency transceiver, such as, for instance, itinerary information collected at each reading of the radiofrequency transceiver. The first and second antennas 106, 107 are planar antennas directly connected to the RFID integrated circuit 105 by conductive paths printed onto the substrate of the RFID inlay 104. The length of the conductive path 120 can be substantially equal to a multiple of half a working wavelength of the radiofrequency transceiver, so as to enhance the range of the radiofrequency transceiver by inductive coupling. For instance, if the working frequency of the radiofrequency transceiver is in the 860-960 MHz band, which corresponds to a wavelength of approximately 0.35 m, the length of the conductive path 120 can be substantially equal to X times 175 mm, wherein X is a whole number equal or higher than one. At such a length, when receiving or transmitting signals at that working frequency, there is inductive coupling between the planar antenna 106 and this electrically conductive path 120, enhancing the range of the radiofrequency transceiver.

[0026] Each one of the first and second electric terminals 117, 118 is also directly connected to the RFID integrated circuit 105 over a conductive path printed onto the substrate of the RFID inlay 104. These first and second electric terminals 117, 118 are shaped as electric

contacts around respective holes in the RFID inlay 104, which are aligned with the channels 111 to allow the introduction of both ends 102a, 102b of the closure element 102 through these holes when received in those channels 111. In order to minimize the bulk and size of the secure sealing device 101, the substrate of the RFID inlay 104 is not flat, but n-shaped, wherein the two electric terminals 117, 118 are located on an intermediate segment 104a of this n-shape, which is oriented in a plane substantially perpendicular to the direction of introduction of both ends 102a, 102b of the closure element 102 through the holes in the RFID inlay 104, and the antennas 106,107 are each to one side of this intermediate segment 104a, on each leg of the n-shape. The antennas 106,107 are thus oriented following two parallel planes which are each at a straight angle to that of the intermediate segment 104a. With this configuration, it is possible to have, within a comparatively thin and compact secure sealing device 101, two antennas 106, 107 of considerable size, each one located to one side of the secure sealing device 101 so as to provide a good coverage in both directions. Moreover, since in this embodiment the two ends 102a, 102b of the closure element 102 are substantially aligned with a plane parallel to those of the two planar antennas 106, 107, the inductive coupling between the conductive path 120 of the closure element 102 and the planar antennas 106,107 is enhanced.

[0027] The RFID integrated circuit 105 may be passive, that is, powered only by the energy of incoming radiofrequency signals, or it may be connected to a power source, such as a battery or capacitor, possibly contained within the secure sealing device 101. This RFID integrated circuit 105 is also configured so as to detect an electric connection between the two electric terminals 117, 118. If the RFID integrated circuit 105 has a rewritable memory and remains connected to a power source, it may also be configured to register, in the rewritable memory, the event of such an electric connection between the terminals 117, 118 and/or its interruption.

[0028] In order to establish an electric connection between these electric terminals 117,118, once the secure sealing element 101 has been closed by inserting both ends 102a,102b of the closure element 102 into the corresponding openings 115 in the locking body 103, sharp edges transverse to the channels 111 within the locking body 103 are configured to locally unsheathe the closure element 102, bringing the electrically conductive path 120 into electric contact with both terminals 117,118. To form the locking body 103, the RFID inlay 104 and locking core 112 may be encased in a dielectric material, such as, for instance a thermosetting or thermoplastic polymer material.

[0029] A method of using the secure sealing device 101 to securely seal a container will now be described with reference to FIG. 1. In use, the elongated, flexible closure member 102 can be threaded and looped around two adjacent elements closing an access to a content to be sealed, such as, for instance, hasps attached to respective wings of a door of a shipping container. In a first step, the secure sealing device 101 is closed by inserting both ends 102a, 102b of the closure element 102 through the corresponding openings 115 into the locking body 103, where they are locked by the holding mechanisms within the locking core 112, irreversibly connecting both ends 102a, 102b of the closure element 102 to the locking body 103, and preventing the separation of the above-mentioned two adjacent elements, so that access to the sealed content is effectively prevented unless the closure element 102 is broken.

[0030] While both ends 102a, 102b of the closure element 102 are locked in place, the sharp edges transverse to the channels 111 partially unsheathe the filaments forming the electrically conductive path 120 at both ends 102a, 102b so as to connect the two electric terminals 117, 118 through this electrically conductive path 120. Once the electric contacts are made, the electric circuit is closed between the two electric terminals 117, 118. If the closure element 102 is cut or pulled by force from the locking body, the RFID integrated circuit 105 will detect this seal breach as an interruption of the connection between the terminals 117, 118. If the RFID integrated circuit 105 is an active circuit with a rewriteable memory, it may even register this event, so as to reveal the breach even if the terminals 117, 118 are subsequently reconnected. The RFID integrated circuit 105 and antennas 106, 107 can be configured so as to communicate with readers at several meters' distance, further enhanced by the inductive coupling between the antennas 106, 107 and the conductive path 120. This allows, for instance, rapid wireless inspection of the seals of shipping containers and trucks by driving them through reader portals. During this inspection, the RFID integrated circuit 105 may transmit, upon being queried by the reader, data stored in its memory to identify the container, its cargo and/or itinerary, but even whether the connection between the terminals 117, 118 has been interrupted at any moment after it was closed, and therefore whether the secure sealing device 101 has been breached. Additionally, the secure sealing device 101 may even comprise a timing and/or positioning device connected to the RFID integrated circuit 105 so as to register not just whether a breach occurred but even when and/or where it occurred. These data may also be transmitted to the reader.

[0031] Even if the RFID integrated circuit 105 is a passive circuit and/or only has a read-only memory, tampering can be prevented by the design of the secure sealing device 101. Because of the shape and construction of the closure element 102, it will be very difficult to reconnect two segments of this closure element 102 after cutting between them, and even more difficult to disguise such a reconnection. If one or both ends 102a, 102b is pulled by force from the locking body 103, the sharp edges having locally unsheathed the conductive path 120 will hold back a whole segment of the sheath 121 within the locking body 103, and subsequently block the reintroduction of that end of the closure element 102. Addition-

ally, the holding mechanisms within the locking core 112 may abrade the sheath 121 as it is pulled through, leaving clear marks on the surface of the sheath 121.

[0032] Moreover, the broken conductive path 120 will not achieve the same inductive coupling with the antennas 106, 107 as an intact conductive path 120, leading to a significant reduction in range which may by itself be detected by the RFID reader. This may be done, for instance, by applying a "power sweep" technique, in which an external reader interrogates the radiofrequency transceiver of the secure sealing device 101 at a given range with a transmission power that is increased gradually or stepwise. If the reader already detects a reply by the radiofrequency transceiver of the secure sealing device 101 in response to an outgoing interrogation signal emitted with a still comparatively low transmission power, this will indicate that said conductive path 120 is still intact, increasing the range and sensitivity of the radiofrequency transceiver of the secure sealing device 101 by inductive coupling. On the other hand, if the reader has to increase the transmission power of the secure sealing device 101 above a predetermined threshold to prompt a detectable response by the secure sealing device 101, this may indicate that the conductive path 120 has been broken, and the secure sealing device 101 breached, prompting thus a close visual inspection of the secure sealing device 101 and/or of the sealed cargo.

[0033] A second, alternative embodiment of a secure sealing device 101 is illustrated in FIGS. 4 and 5. The same reference numbers as for the components of the first embodiment are used for the analogous components of the second embodiment. This second embodiment differs from the first embodiment in that the second end 102b of the closure element 102 is solid with the locking body 103, with the electrically conductive path 120 fixedly connected to the second terminal 118. The locking core 112 thus only has a single holding mechanism, configured so as to hold the first end 102a of the closure element 102 when it is introduced in the channel 111 leading to the first terminal 117. In use, this secure sealing device 101 works analogously to that of the first embodiment. The same power sweep technique may be used to determine a breach of this secure sealing device 101.

[0034] A secure sealing device 101 according to a third embodiment of the present invention is illustrated in FIGS. 6 and 7. The same reference numbers as for the components of the first and second embodiment are used for the analogous components of this third embodiment. This secure sealing device 101 is similar to that of the first embodiment, except in particular in that the electrically conductive path 120 of the closure element 102 is not sheathed, but exposed instead. Furthermore, in this third embodiment, as illustrated on FIG. 7, the RFID inlay 104 does not present any electric terminals configured to contact this electrically conductive path 120, which instead contacts the metallic locking core 112 at both ends 102a, 102b of the closure element 102. Consequently, there isn't, in this embodiment, any provision for the active detection and storage of a breach of the secure sealing device 101 by the RFID integrated circuit 105. However, because the length of the conductive path 120 is substantially equal to a multiple of half a working wavelength of the radiofrequency transceiver, the closed loop formed by the intact conductive path 120 and the metallic locking core 112 can significantly increase the range of the radiofrequency transceiver. The corresponding decrease in this range in case of a breach of the secure sealing device 101 breaking the conductive path 120 can be detected by an RFID reader during remote inspection of the secure sealing device 101 using the abovementioned power sweep technique, alerting to such tampering.

[0035] A secure sealing device 101 according to a fourth embodiment of the present invention is illustrated in FIGS. 8A, 8B and 9. As can be seen in FIG. 8A, this secure sealing device 101 comprises a closure element 102 in the form of a plastic ratchet strap, and a locking body 103 integrally formed with the closure element 102. A first end 102a of this closure element 102a is free, whereas a second end 102b is fixedly connected to the locking body 103. The locking body 103 presents an opening 115 for receiving the first end 102a of the closure element 102 to close the secure sealing device 101. Within the opening 115, a holding mechanism 116 is shaped so as to allow the introduction of the closure element 102 through the opening 115 in one direction, but cooperate with the ratchet teeth 102c to prevent its subsequent retreat in the opposite direction. This holding mechanism can be reinforced to ensure that, under a pulling force, the closure element 102 will break before the irreversible connection between the lock body 103 and the first end 102a of the closure element 102. In the illustrated embodiment, the lock body 103 forms a tag which can present visible markings (not shown), in the form, for instance, of alphanumeric codes, bar codes, or other human- or machine-readable codes, printed or embossed, or of other authentication or identification markings, such as, for instance, holograms.

[0036] As illustrated in the cutaway view of FIG. 8B, the secure sealing device 101 also comprises, embedded within the locking body 103, an RFID inlay 104 carrying an electric circuit comprising a data carrier, a transceiver, and first and second antennas 106,107 for the transceiver. In this fourth embodiment, the data carrier and transceiver are also integrated in a RFID integrated circuit 105, compliant with ISO/IEC 18000. The working frequencies of this RFID integrated circuit 105 may also be, for instance, 2.45 GHz, as specified under ISO/IEC 18000-4, 860-960 MHz, as specified under ISO/IEC 18000-6, and/or 433 MHz, as specified under ISO/IEC 18000-7. In particular, in this fourth embodiment, the RFID integrated circuit may be configured so as to use a plurality of different frequencies. As in the other embodiments, the data carrier can be a read-only or a rewritable memory, wherein a rewritable memory could store information received by the radiofrequency trans-

ceiver, such as, for instance, itinerary information collected at each reading of the radiofrequency transceiver. The substrate of the RFID inlay 104 is also n-shaped, and the antennas 106,107 formed on two lateral segments 104b, 104c oriented following two parallel planes, each at a straight angle to the plane of the intermediate segment 104a.

[0037] The secure sealing device 101 also comprises a plurality of parallel conductive paths 120 of different lengths in the closure element 102, printed on a non-conductive substrate of the secure sealing device 101. This non-conductive substrate can be produced, for instance, in a first injection molding step, and the RFID inlay 104 and plurality of parallel conductive paths 120 can be safely encapsulated in a subsequent second injection molding step. The length of each conductive path 120 can be substantially equal to a multiple of half a working wavelength of the radiofrequency transceiver. For instance, if the radiofrequency transceiver has a first working frequency in the 860-960 MHz band, and a second working frequency around 433 MHz, which correspond, respectively, to a first wavelength of approximately 0.35 m and a second wavelength of 122 mm, the length of a first conductive path 120 can be substantially equal to X times 175 mm, and that of a second conductive path 120 substantially equal to Y times 61 mm, wherein X and Y are whole numbers equal or higher than one. With such lengths, when receiving or transmitting signals at one of these working frequencies, there is inductive coupling between the planar antennas 106, 107 and the corresponding electrically conductive path 120, enhancing the range of the radiofrequency transceiver.

[0038] In use, the elongated, flexible closure member 102 can be threaded and looped around two adjacent elements closing an access to a content to be sealed, such as, for instance, hasps attached to respective wings of a door of a shipping container. The second end 102b of the closure member 102 is then threaded through the opening 115, irreversibly connecting it to the locking body 103, and preventing the separation of the abovementioned two adjacent elements, so that access to the sealed content is effectively prevented unless the closure member 102 is broken.

[0039] If the closure member 102 is broken, the conductive paths 120 are also broken, and the range of the radiofrequency transceiver decreased, as in the third embodiment. It must be noted that, because the electrically conductive path 120 is embedded within the closure member 102, it will normally not be possible to reliably re-establish this electrically conductive path 120 by repairing the broken closure member 102.

[0040] If the radiofrequency transceiver 105 is interrogated by a remote reader, the range at which it will be able to respond to an interrogation signal at a given transmission power will thus depend on the state of the closure member 102. The abovementioned power sweep technique may thus be used to determine whether a closer inspection of the secure sealing device 101 is appropriate. The visible markings in the locking body 103 can then complement the information provided by the radiofrequency transceiver 105.

[0041] Those skilled in the art will recognize that the present invention may be manifested in a variety of forms other than the specific embodiments described and contemplated herein. In particular, other embodiments may combine individual features of the four embodiments disclosed. Accordingly, departure in form and detail may be made without departing from the scope of the present invention as described in the appended claims.

Claims

1. Secure sealing device (101) comprising at least :

   a closure element (102) with at least one electrically conductive path (120) ;
   a locking body (103) comprising an electric circuit with a data carrier and a radiofrequency transceiver with a predetermined working wavelength, said locking body (103) being configured to lock together a first and a second end (102a,102b) of said closure element (102) to attach the locking body (103) to an object to be sealed ; and
   the secure sealing device (101) being **characterized in that** said at least one electrically conductive path (120) of the closure element (102) has a length which is substantially equal to a multiple of half said predetermined working wavelength of the radiofrequency transceiver.

2. Secure sealing device (101) according to claim 1, wherein said electric circuit further comprises at least a first planar antenna (106) oriented in a first plane and connected to said radiofrequency transceiver, and wherein said locking body (103) is configured to lock together said first and second ends (102a,102b) of the closure element oriented in a plane substantially parallel to said first plane.

3. Secure sealing device (101) according to claim 2, wherein said electric circuit further comprises at least a second planar antenna (107) oriented substantially parallel to the first planar antenna (106).

4. Secure sealing device (101) according to any one of claims 1 to 3, wherein said electric circuit comprises first and second electric terminals (117,118) configured to be connected through the electrically conductive path (120) of the closure element (102) when the first and second ends (102a,102b) of the closure element (102) are locked together by the locking body (103).

5. Secure sealing device (101) according to claim 4,

wherein the electric circuit is configured to automatically store within said data carrier whether a connection between said first and second electric terminals (117,118) has been interrupted.

6. Secure sealing device (101) according to any one of claims 4 or 5, wherein the electric circuit is formed onto a substrate comprising at least a first segment, incorporating at least a first planar antenna (106) of the radiofrequency transceiver, extending in a first plane, and a second segment, supporting at least said first and second terminals (117,118) and extending in a second plane at an angle, for example a substantially straight angle, with respect to the first plane.

7. Secure sealing device (101) according to claim 6, wherein said substrate further includes a third segment, supporting at least a second planar antenna (107) of the radiofrequency transceiver, and extending substantially parallel to the first segment.

8. Secure sealing device (101) according to any one of claims 1 to 7, wherein said electric circuit is encased within a dielectric material.

9. Secure sealing device (101) according to any one of the preceding claims, wherein said locking body (103) comprises at least a first opening (115) for insertion of the first end (102a) of said closure element into said locking body (103), and a first holding mechanism for preventing removal of said first end (102a) from said first opening (115) once inserted.

10. Secure sealing device (101) according to claim 9, wherein said locking body (103) comprises a second opening (115) for insertion of the second end (102b) of said closure element (102) into said locking body (103), and a second holding mechanism for preventing removal of said second end (102b) from said second opening (115) once inserted.

11. Secure sealing device (101) according to claim 9, wherein said second end (102b) of said closure element (102) is solid with said locking body (103).

12. Secure sealing device (101) according to any one of the preceding claims, wherein the closure element (102) is flexible.

13. Secure sealing device (101) according to any one of claims 1 to 12, wherein said radiofrequency transceiver has a plurality of predetermined working wavelengths, and said closure element (102) has a plurality of electrically conductive paths (120) of different lengths, each one substantially equal to a multiple of one half of one of said plurality of predetermined working wavelengths of the radiofrequency transceiver.

14. A method for checking a secure sealing device (101) according to any one of claims 1 to 13, wherein an external reader, located at a predetermined range from said radiofrequency transceiver, sends an interrogation signal, addressed to the radiofrequency transceiver and using said working wavelength, at various different transmission power levels, and issues an alert if it fails to receive a response of the radiofrequency transceiver below a predetermined transmission power threshold of the interrogation signal.

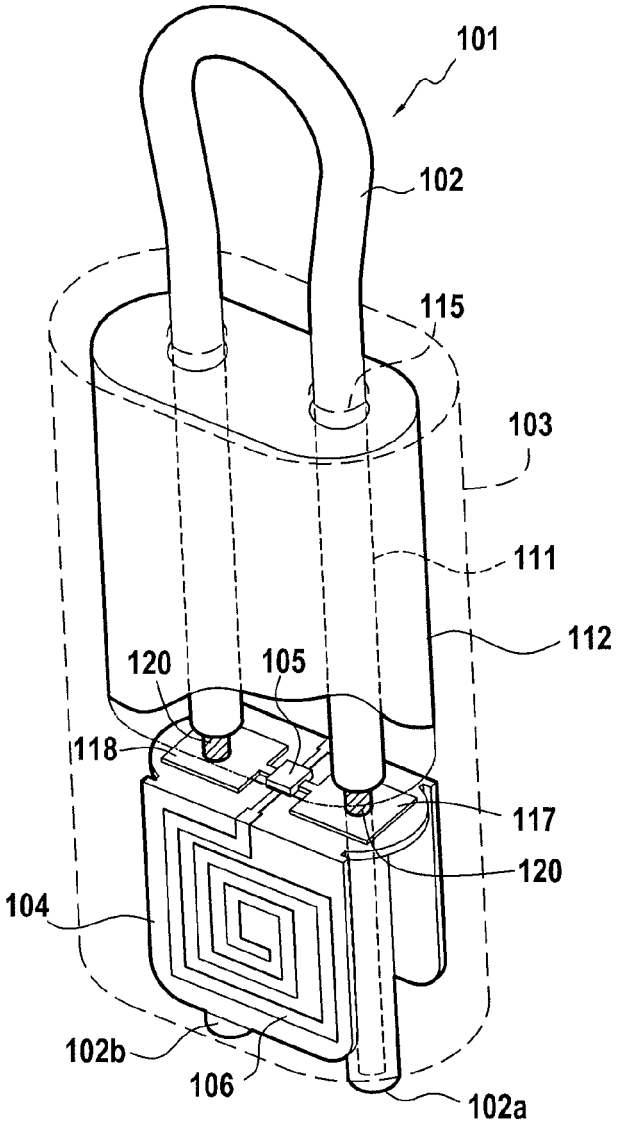


FIG.1

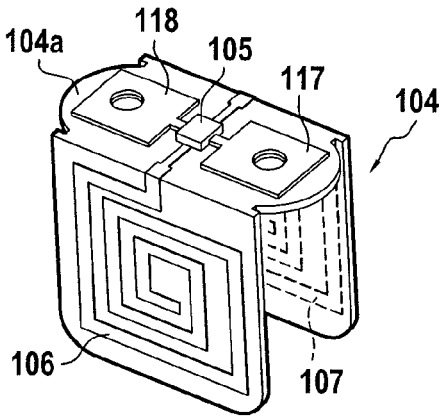


FIG.2

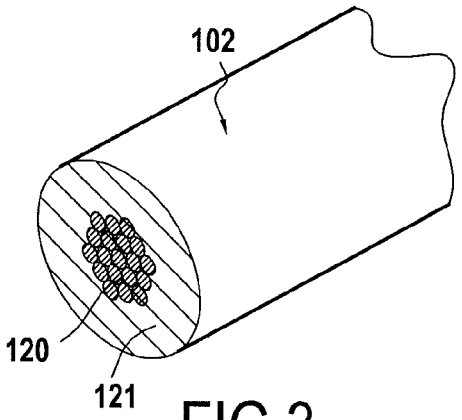


FIG.3

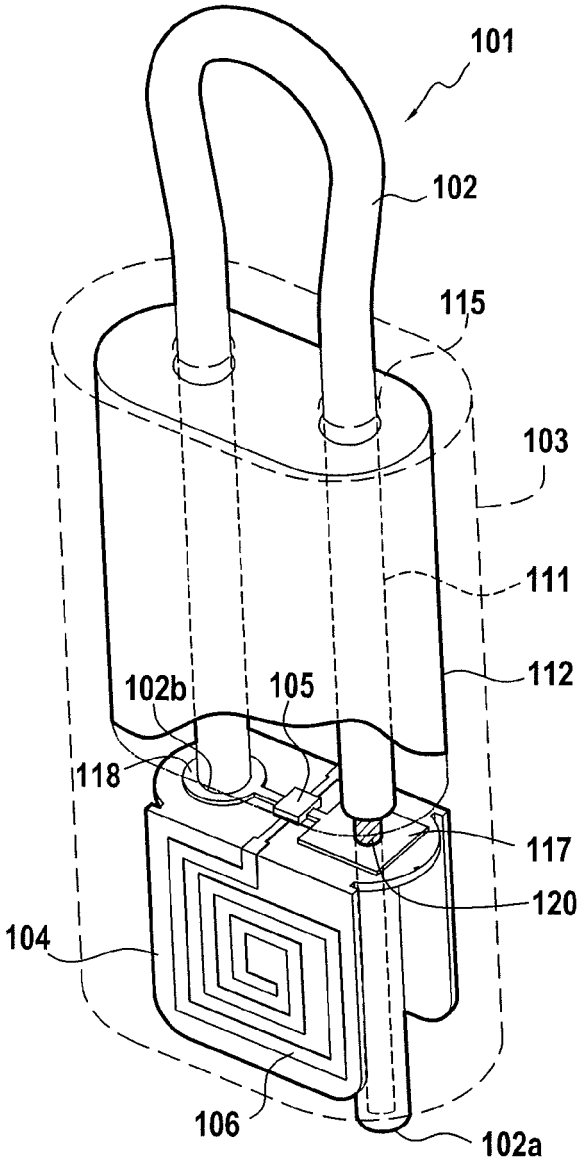

101
102
115
103
111
112
102b
105
118
117
120
104
106
102a

FIG.4

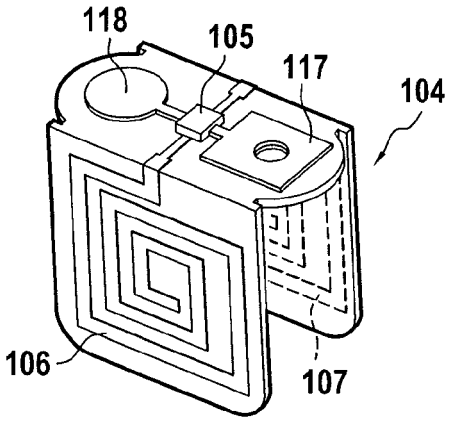
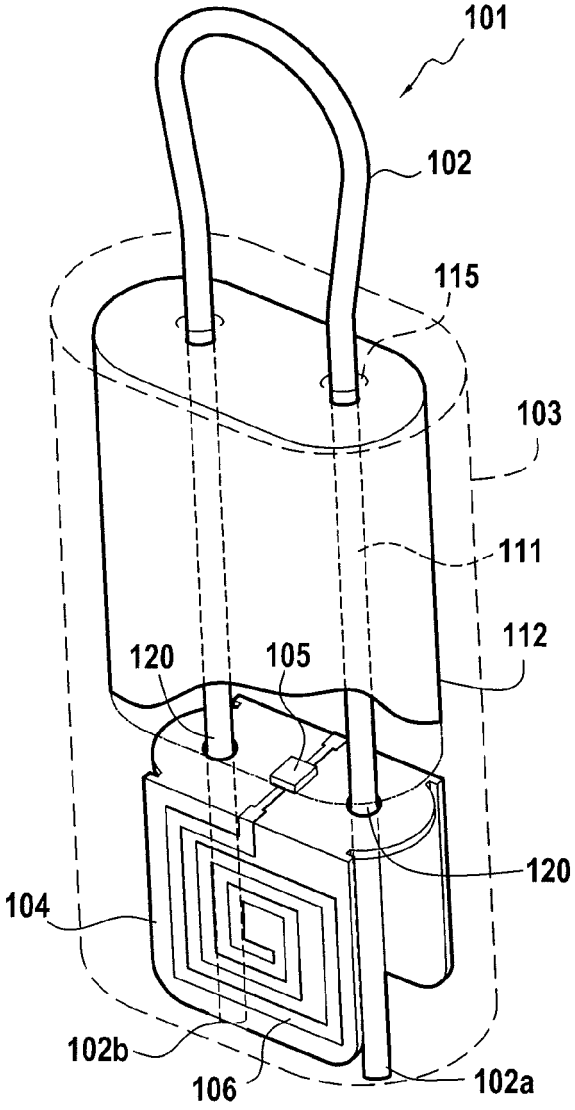

118
105
117
104
106
107

FIG.5

FIG.6


101
102
115
103
111
112
120
105
120
104
102b
106
102a

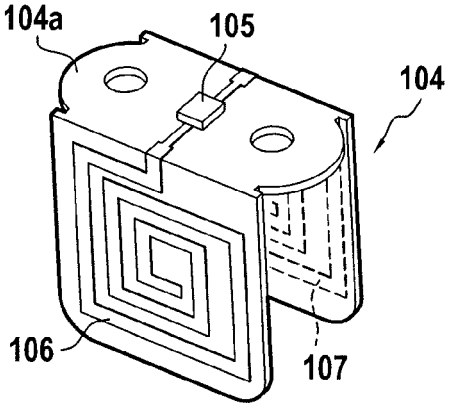

104a
105
104
106
107

FIG.7

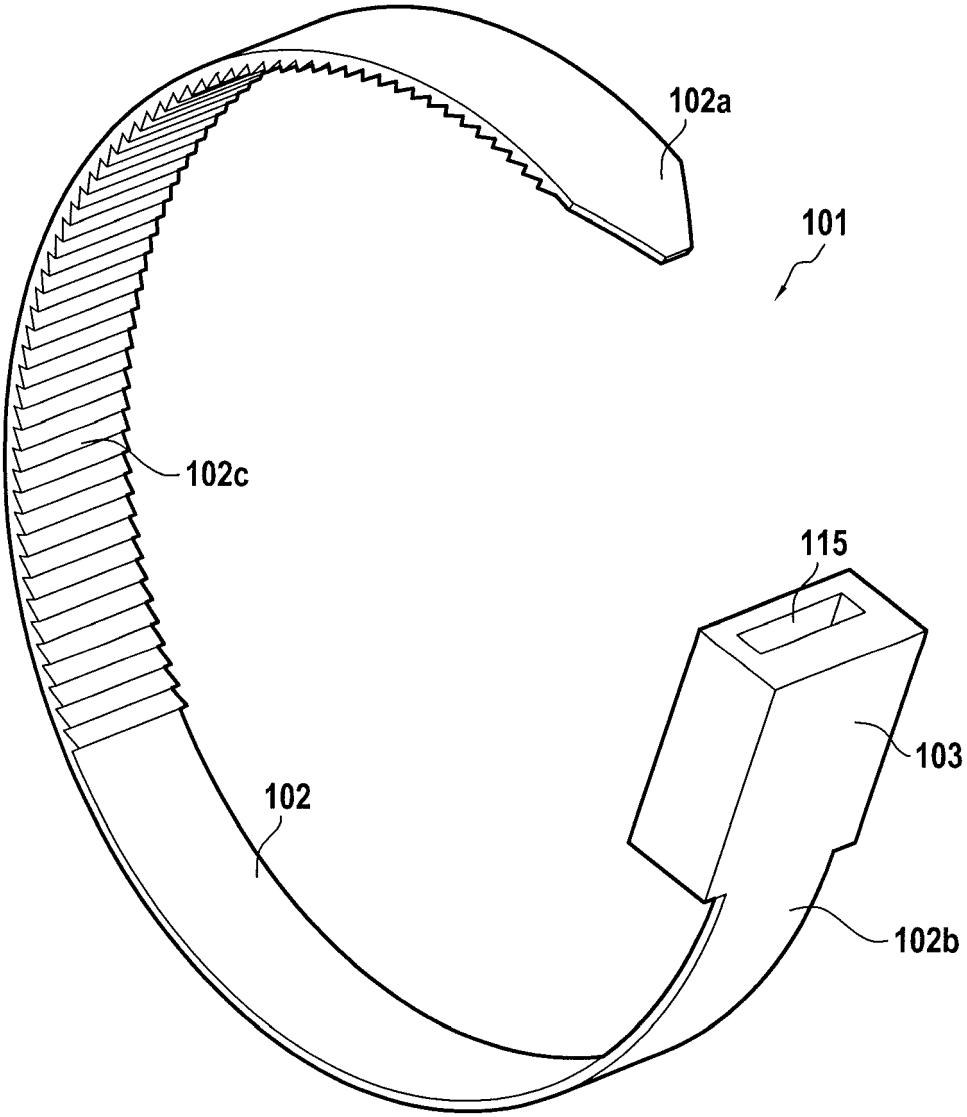
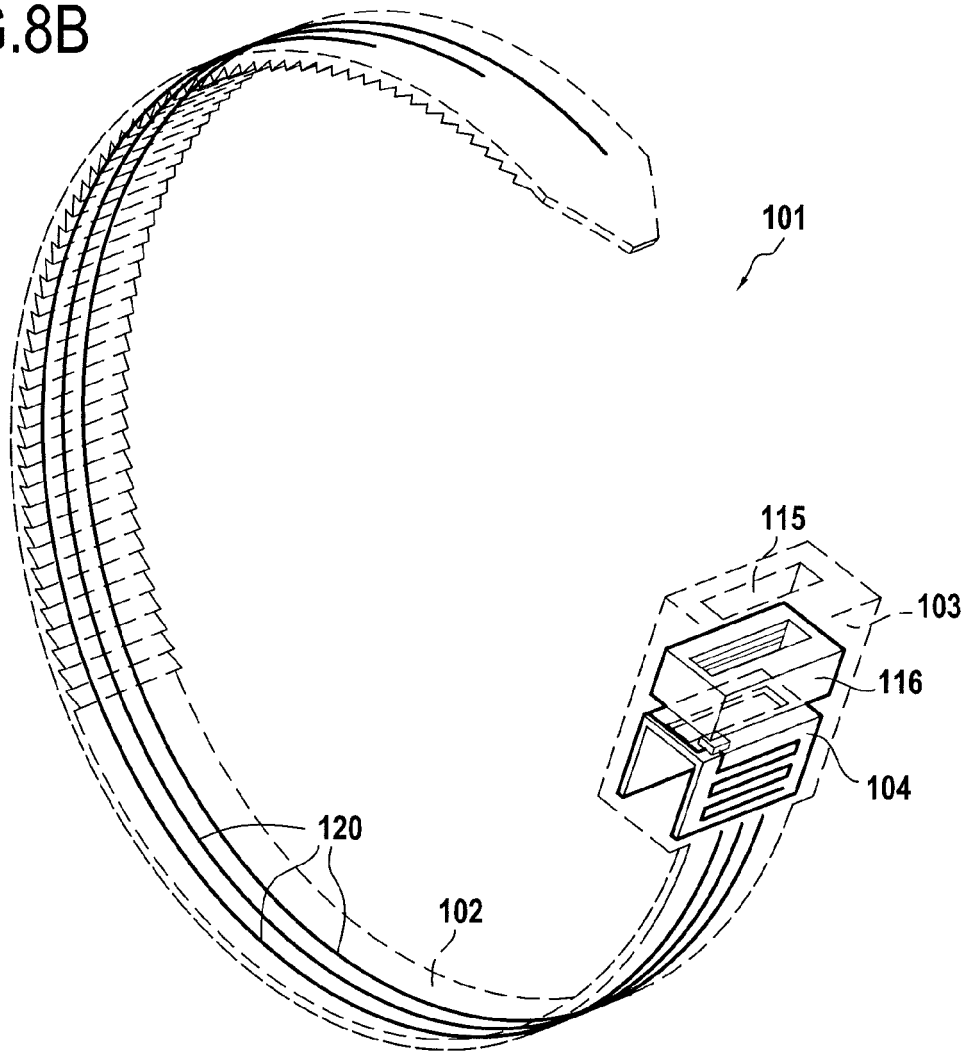


FIG.8A

FIG.8B



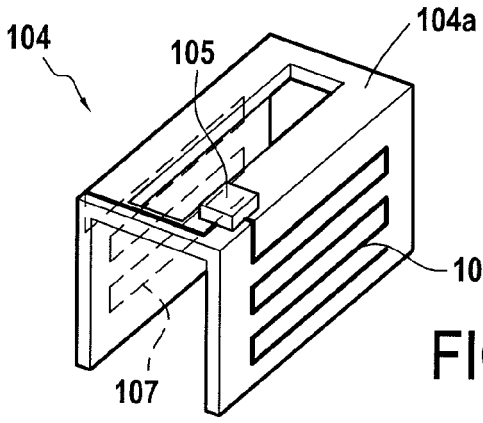


FIG.9

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 12 19 7521

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	DE 10 2004 063487 A1 (INTEC HOLDING GMBH [DE]) 13 July 2006 (2006-07-13) * paragraphs [0043], [0046]; figures 8,10 * -----	1-14	INV. G06K19/077 G09F3/03
A,D	US 2005/231365 A1 (TESTER THEODORE R [US] ET AL) 20 October 2005 (2005-10-20) * abstract * -----	1-14	

TECHNICAL FIELDS SEARCHED (IPC)

G06K
G09F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	29 April 2013	Schmidt, Rainer

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 12 19 7521

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

29-04-2013

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 102004063487 A1	13-07-2006	AT 498173 T	15-02-2011
		CN 101142606 A	12-03-2008
		DE 102004063487 A1	13-07-2006
		EP 1831862 A1	12-09-2007
		ES 2360295 T3	02-06-2011
		JP 4792041 B2	12-10-2011
		JP 2008525675 A	17-07-2008
		US 2007139196 A1	21-06-2007
		WO 2006066555 A1	29-06-2006
US 2005231365 A1	20-10-2005	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 20050231365 A1 **[0005]**
- US 20070103310 A1 **[0005]**
- US 6265973 B1 **[0005]**
- US 20060145868 A1 **[0006]**
- US 20060087431 A1 **[0006]**
- US 20070139196 A1 **[0006]**